513-CD-001-002

EOSDIS Core System Project

Hazard Analyses for the ECS Project

Final

March 1995

Hughes Applied Information Systems
Landover, Maryland

Hazard Analyses for the ECS Project

Final

March 1995

Prepared Under Contract NAS5-60000
CDRL Item 086

SUBMITTED BY

Peter G. O'Neill /s/ for	3/17/95
Marshall A. Caplan, Project Manager EOSDIS Core System Project	Date

Hughes Applied Information Systems
Landover, Maryland

513-CD-001-002

This page intentionally left blank.

Preface

This document is a formal contract deliverable with an approval code 2. As such, it does not require formal Government approval, however, the Government reserves the right to request changes within 45 days of the initial submittal or any subsequent revision. Changes to this document shall be made by document change notice (DCN) or by complete revision.

Once approved, this document shall be under the ECS Project Configuration Control. Any questions should be addressed to:

Data Management Office
The ECS Project Office
Hughes Applied Information Systems
1616 McCormick Dr.
Landover, MD 20785

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Final
iii through viii	Final
1-1 and 1-2	Final
2-1 and 2-2	Final
3-1 and 3-2	Final
4-1 and 4-2	Final
5-1 and 5-2	Final
AB-1 and AB-2	Final

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
513-CD-001-001 513-CD-001-002	Review Copy Final	February 1995 March 1995	

This page intentionally left blank.

Contents

This page intentionally left blank.

1. Introduction

1.1 Identification

This document is submitted as required by CDRL Item 086, DID 513/PA2, whose requirements are specified in this document as a deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS) Contract (NAS5-60000).

1.2 Scope

There are three aspects of hazard analysis considered in this document: ground system hazard analysis, spacecraft hazard analysis, and the loss of mission essential data.

The ground system hazard analysis identifies both hardware and software caused hazards for each Element and Segment of the ECS. Hazards to ECS personnel and equipment as well as potential hazards external to ECS is also considered.

The spacecraft hazard analysis is limited to the Flight Operations Segment (FOS). In the software area, the analysis focuses on mission critical items and examines potential malfunctions that can result in damage to, or loss of, flight hardware or the mission, including loss of critical science data.

This document reflects the Technical Baseline submitted via contract correspondence no. ECS 194-00343.

1.3 Purpose and Objectives

The purpose of this document is to provide high level hazard analysis results of the ECS as described in the Data Item Description of DID 513/PA2 and to provide pointers to existing ECS hazard analysis related documents and plans that have documented current and future hazard protection and mitigation activities.

1.4 Document Status and Schedule

This submittal of DID 513/PA2 meets the milestone specified in the Contract Data Requirements List (CDRL) of NASA contract NAS5-60000.

The next updated version of the Hazard Analyses will be submitted two weeks prior to each release's Incremental Design Review (IDR).

1.5 Document Organization

The document is organized into five (5) sections, Abbreviations and Acronyms and one Appendix:

Section 1	Introduction, contains the identification, scope, purpose and objectives, status and schedule, and document organization.
Section 2	Related Documentation, provides a bibliography of parent, applicable and information documents for the Hazard Analysis.
Section 3	Ground System Hazard Analysis, provides a brief description of existing hazard mitigation documents for ground COTS hardware.
Section 4	Spacecraft Hazard Analysis, provides a summary of existing spacecraft hazard related analysis documents.
Section 5	Loss Of Mission Essential Data Analysis, provides a high level data capture analysis.
Appendix A Abbreviations and Acronyms.	

2. Related Documentation

2.1 Parent Documents

The parent document is the document from which this Hazard Analyses document scope and content are derived.

194-207-SE1-001	Systems Design Specification for the ECS Project
420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System
423-41-03	Goddard Space Flight Center, EOSDIS Core System (ECS) Contract Data Requirements Document

2.2 Applicable Documents

The following documents are referenced within this Hazard Analyses document, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume.

194-501-PA1-001	Performance Assurance Implementation Plan for the ECS Project

2.3 Information Documents

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the Hazard Analyses document.

194-219-SE1-001	Interface Requirements Document Between EOSDIS Core System (ECS) and the NASA Science Internet (NSI)
194-302-DV2-001	ECS Facilities Plan for the ECS Project
305-CD-002-001	Science Data Processing Segment (SDPS) Design Specification for the ECS Project, Review Copy
517-CD-001-002	Failure Modes and Effects Analyses (FMEA) and Critical Items List (CIL), Final

520-CD-001-001	Software Critical Items List
613-CD-001-001	COTS Maintenance Plan for the ECS Project, Preliminary
622-CD-001-001	Training Plan for the ECS Project

3. Ground System Hazard Analysis

The ground system hazard analysis considered both hardware and software caused hazards for each Element and Segment of ECS. The analysis considered hazards to ECS personnel and to the ECS equipment, and potential hazards external to ECS.

This analysis concluded that the effect of ongoing and future planning and implementation processes to purchase, verify, integrate and test, install, operate and maintain COTS hardware minimizes the potential for a ground system hazardous condition to personnel or equipment. These various processes and the documents that describe them are:

- Procurement of COTS hardware to commercial practice UL performance and safety standards. Other commercial standards such as ANSI, BICSI, CCITT, EIA, IEEE, ISO, and NEC may also be applicable. The COTS hardware installed in the user environment has been engineered for the user desktop operating environment with enclosed components and no exposure to moving parts or electrical discharge. The COTS hardware installed in the data center environment will be accessible only to authorized, trained and certified operators and maintainers.
- Installation and Facility Planning to provide the DAACs with site specific Installation Plans and the ECS Facilities Plan (DID 302) to provide the planning necessary to assure that each ECS component will meet all requirements for interfacing with the facilities in which they are located. The Facilities Plan will contain physical layout, electrical power requirements, air conditioning requirements, antenna foundation, final equipment layout, mechanical/electrical loads, and functional arrangements.
- Environmental Control Planning to identify, in the Environmental Control Plan (DID 532), suitable environmental and cleanliness controls for all areas used for the operation, storage, maintenance, repair, inspection, or test of system equipment.
- Maintenance Planning, in the COTS Maintenance Plan (DID 613), to describe policies and procedures to be applied to maintenance of all hardware and software under M&O responsibility.
- M&O Procedures and the Operational Readiness Plan (DID 603) to describe the processes to assure all elements are in a state of operational readiness at all times.
- M&O Personnel Certification and Training to define the certification and COTS training required to prepare personnel to operate, maintain, and use the ECS. The COTS Training Plan (DID 622) and the M&O Certification Plan (DID 626) detail the approach and procedures required.
- Security Planning documents the approach to physical, informational and personnel security in the ECS Security Plan (DID 214).
- Disaster Recovery and Emergency Preparedness Planning is contained in the EDF Disaster Recovery Plan which provides for the safety and the protection of HAIS and the safeguarding of NASA computer resources and data assets. The Emergency Preparedness Plan focuses on personnel, visitors, and non-data assets.

This page intentionally left blank.

4. Spacecraft Hazard Analysis

The Spacecraft Hazard Analysis is limited to the Flight Operations Segment (FOS). In the software area the analysis focused on the mission critical items, as well as the spacecraft hazardous command loads. It examined the potential malfunctions/hazards that can result in damage to or loss of the flight hardware or the mission, including the loss of critical science data.

The software analysis and identified critical items are contained in DID 520, the Software Critical Items List. This document provides analyses of potential hazards that may be caused by the identified software critical items as well as a hazard mitigation plan for each identified item.

The hardware analysis has been conducted for the FOS Critical Real-Time Command and Control functions and has been documented in detail in DID 517, Failure Modes and Effects Analysis (FMEA). The FMEA results revealed that there are no critical hardware items identified for the above function due to the FOS robust design with end-to-end redundant architecture.

This page intentionally left blank.

5. Loss Of Mission Essential Data Analysis

Mission essential data will be first captured by the EDOS Data Ingest Facility (DIF) and then transferred to EDOS Data Production Facility (DPF) for long term archiving. The media library at the DIF stores the physical media necessary for controlling all operations and the short-term raw data recordings of the return link mission data recorded by the data capture function. The short-term raw data recordings of return-link mission data will be archived for at least 30 days. All raw data recordings will be logged in, stored sequentially on storage shelves, removed for recycling, and logged out when recycled. The logs will be retained indefinitely.

The data from the DPF will then be transferred to the Ingest Subsystem of the ECS Science Data Processing Segment (SDPS) within 24 hours or less. Typically, data transfer must be completed within several hours to free up resources at the Level 0 processing sites or DPFs, as new data sets are being received on a nearly continuous basis. The EDOS Level 0 processing sites provide long term archive of mission essential data, in conjunction with the Ingest Subsystem, in the event that data is corrupted or lost in the transfer to ECS or within ECS itself .

The Ingest Subsystem of the SDPS will be designed to meet stringent Operational Availability (A_O) and Mean Down Time (MDT) requirements of 0.999 and 2 hours respectively. This will be achieved with a standby redundant ingest client host, redundant archive storage and reliable archive component architecture. Hot and warm spare backups will be provided to the working storage and Level 0 data server media drive and robotics devices. For more details of the Ingest Subsystem design refer to the SDPS Segment/Element Design Specifications, document number 305-CD-002-001.

This high level analysis concluded that there is sufficient redundancy in the capture, handling, and processing of science data to mitigate the risk of loss of this data.

This page intentionally left blank.

Abbreviations and Acronyms

ANSI	American National Standards Institute
A_O	Operational Availability
BICSI	Building Industry Consulting Service International
CCITT	International Telegraph & Telephone Consultative Committee
CIL	Critical Items List
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Data Requirements List
COTS	Commercial Off The Shelf
DAAC	Distributed Active Archive Center
DCN	Document Change Notice
DID	Data Item Description
DIF	Data Ingest Facility
DPF	Data Production Facility
ECS	EOSDIS Core System
EDF	ECS Development Facility
EDOS	EOS Data and Operations System
EIA	Electronics Industry Association
EOS	Earth Observing System
EOSDIS	Earth Observing System Data and Information System
FMEA	Failure Modes & Effects Analysis
FOS	Flight Operations Segment (ECS)
HAIS	Hughes Applied Information Systems
IDR	Incremental Design Review
IEEE	Institute of Electrical and Electronics Engineers, Inc.
ISO	International Organization for Standardization
M&O	Maintenance and Operations
MDT	Mean Down Time

NASA	National Aeronautics and Space Administration
NEC	National Electric Code
NSI	NASA Science Internet
PDR	Preliminary Design Review
SDPS	Science Data Processing Segment (ECS)
UL	Underwriters Laboratory